

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.В.06
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Технологии и методы социальной инженерии

(наименование дисциплины)

по направлению подготовки
09.03.03 Прикладная информатика

направленность (профиль)
Прикладная информатика в информационной безопасности

Форма обучения: очная

Год набора: 2026

Общая трудоемкость: 43Е

Распределение часов дисциплины по семестрам

Семестр	6	Итого
Форма контроля	зачет	
Вид занятий		
Лекции	16	16
Лабораторные	-	-
Практические	32	32
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0.25	0.25
Контактная работа	48,25	48,25
Самостоятельная работа	95,75	95,75
Контроль	-	-
Итого	144	144

Рабочую программу составил(и):

Доцент ИИиЭБ, к.э.н., доцент, Фрезе Т.Ю.

(должность, ученое звание, степень, Фамилия И.О.)

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:



Отсутствует



Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана направления подготовки (специальности) 09.03.03 Прикладная информатика

Срок действия рабочей программы дисциплины до 31.08.2030

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности

(протокол заседания № 1 от 01.09.2025).

1. Цель освоения дисциплины

Целями освоения дисциплины «Технологии и методы социальной инженерии» являются овладение методами системного анализа процессов, тактик и техник нарушителей, с целью их выявления, последующей нейтрализации, основами нейролингвистического программирования, а также овладение навыками работы с пользователями информационных систем в области повышения осведомленности с методами работы социальных инженеров.

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина: Основы управления информационной безопасностью; Комплексная безопасность.

Дисциплины и практики, для которых освоение данной дисциплины необходимо как предшествующее: Мониторинг событий информационной безопасности.

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
ПК-9 Способен формулировать политики информационной безопасности	ПК-9.1 Использует принципы построения и развития социальной инженерии, основы теории системного подхода при решении задач защиты информации	Знать: - принципы построения и развития социальной инженерии, основы теории системного подхода при решении задач защиты информации; -основные особенности, принципы и методы социальной инженерии, показатели и критерии эффективности применения методов;
		Уметь: - находить и использовать информацию, необходимую для ориентирования в текущих задачах информационной безопасности
		Владеть: - основами социальной инженерии
	ПК-9.2 Умеет провести оценку проблемной ситуации в сфере социальной инженерии, выявить основные	Знать: - основные тенденции совершенствования социальной инженерии Уметь:

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
	закономерности и тенденции применения форм и методов нарушителями	- провести оценку проблемной ситуации в сфере социальной инженерии
		Владеть: - методами работы нарушителей с целью их выявления и нейтрализации
	ПК-9.3 Владеет основами соц инженерии, методами работы нарушителей с целью их выявления и нейтрализации	Знать: - методы нарушителей по воздействию на объекты внимания. - техники СИ, виды атак
		Уметь: - установить и настроить DLP систему Владеть: - навыками применения DLP

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 1 Социальная инженерия (СИ) как система манипуляций	Лек	1.1 Введение в СИ, научные основы, почему работает, точки воздействия	6	2	-	-	Банк тестовых заданий
	Лек	1.2 Слабости психики, принципы/стереотипы, мотивы/страхи, модели, защита	6	2	-	-	Банк тестовых заданий
	Пр	Практическая работа 1 Хронологии развития социальной инженерии	6	2	-	-	Отчет по практической работе
	Пр	Практическая работа 2 Оценка личной уязвимости к социальной инженерии	6	2	-	-	Отчет по практической работе
	Пр	Практическая работа 3 Принципы влияния Р. Чалдини в социальной инженерии	6	2	-	-	Отчет по практической работе
	Ср	Самостоятельное изучение материала, чтение электронного учебника	6	15.75		-	Банк тестовых заданий
Модуль 2. Разведка и сбор информации	Лек	2.1. Разведка и сбор информации в социальной инженерии	6	2	-	-	Банк тестовых заданий
	Пр	Практическая работа 4 Введение в OSINT: цифровой след человека	6	2	-	-	Банк тестовых заданий

	Пр	Практическая работа 5 Анализ специализированных OSINT-инструментов: классификация, функционал и сценарии применения	6	4	-	-	Отчет по практической работе
	Пр	Практическая работа 6 Моделирование цикла атаки Hadnagy	6	2	-	-	Отчет по практической работе
	Пр	Практическая работа 7 Введение в Sherlock: автоматизированный поиск аккаунтов по никнейму	6	4	-	-	Отчет по практической работе
	Пр	Практическая работа 8 Визуальный OSINT-анализ с Maltego Community Edition	6	4	-	-	Отчет по практической работе
	Пр	Практическая работа 9. Автоматизация OSINT-расследований с использованием больших языковых моделей (LLM): от промпт-инжиниринга до аналитического отчета»	6	2	-	-	Отчет по практической работе
	Ср	Самостоятельное изучение материала, чтение электронного учебника	6	20		-	Банк тестовых заданий
Модуль 3. Методы атаки и используемые технические средства	Лек	3.1 Фишинг, вишинг, Evil Twin WiFi.	6	2	-	-	Банк тестовых заданий
	Лек	3.2 Дубликаты аккаунтов/Takeover, дипфейки, ИИ-инструменты, физическое проникновение	6	2	-	-	Банк тестовых заданий
	Пр	Практическая работа 10. Моделирование атаки Evil Twin WiFi и анализ	6	2	-	-	Отчет по практической работе

		безопасности беспроводных сетей					
	Пр	Практическая работа 11. Разработка сценария комплексной атаки с использованием методов социальной инженерии	6	2	-	-	Отчет по практической работе
	Ср	Самостоятельное изучение материала, чтение электронного учебника	6	20		-	Банк тестовых заданий
Модуль 4. Способы противодействия методам социальной инженерии	Лек	4.1 Способы противодействия методам социальной инженерии	6	2	-	-	Банк тестовых заданий
	Пр	Практическая работа 12 Анализ 50 постов о компании. Выявление уязвимостей	6	2	-	-	Отчет по практической работе
	Ср	Самостоятельное изучение материала, чтение электронного учебника	6	20		-	Банк тестовых заданий
Модуль 5. Тестирование на проникновение и повышение осведомленности	Лек	5.1 Подготовка легитимной атаки (юридические аспекты, профайлинг, методология).	6	2	-	-	Банк тестовых заданий
	Лек	5.2 Тестирование инструментов, проведение атаки, отчеты, повышение осведомленности	6	2	-	-	Банк тестовых заданий
	Пр	Практическая работа 13. Оценка уровня защищенности организации от социальной инженерии	6	2			Отчет по практической работе
	Ср	Самостоятельное изучение материала, чтение электронного учебника	6	20			Банк тестовых заданий

	ПА	Промежуточная аттестация/ Итоговое тестирование	5	0,25		-	Банк тестовых заданий /Вопросы к зачету
Итого:				144			

5. Образовательные технологии

Технология	Формы обучения	Методы обучения
Технология традиционного обучения – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Лекция. Практическое занятие. Самостоятельная работа. Индивидуальное домашнее задание.	Наглядные, словесные, практические.
Технология модульного обучения – организация учебного процесса для полного овладения содержанием образовательных программ на основе независимых учебных модулей с учетом индивидуальных интересов и возможностей субъектов образовательного процесса.	Лекция-консультация. Семинар с использованием метода анализа конкретных ситуаций.	Решение ситуационных задач. Презентационный метод. Самостоятельная работа. Консультация. Индивидуальная работа.
Информационные технологии – специальные способы, программные и технические средства (кино, аудио – и видеосредства, компьютеры) для работы с информацией	Лекция-пресс-конференция. Визуальная лекция.	Презентационный метод.
	Формы и методы обучения	
Дистанционное обучение	Сетевая технология – изучение курса (учебной дисциплины) посредством электронных учебно-методических материалов, размещенных в обучающей среде с использованием компьютера, подключенного к сети Интернет. CD-технология – изучение курса (учебной дисциплины), представленного студенту в виде автономной электронной обучающей системы и электронной версии учебно-методических материалов на CD-диске.	

6. Методические указания по освоению дисциплины

6.1. Рекомендации по освоению лекционного материала, подготовке к лекциям

Лекции являются одним из основных видов учебных занятий в высшем учебном заведении. В ходе лекционного курса проводится изложение современных научных материалов в систематизированном виде, а также разъяснение наиболее трудных вопросов учебной дисциплины. При изучении дисциплины следует помнить, что лекционные занятия являются направляющими в большом объеме научного материала. Большую часть знаний студент должен набирать самостоятельно из учебников и научной литературы. Конспекты лекций рекомендуется использовать при подготовке к лабораторным занятиям, экзамену, контрольным тестам, при выполнении самостоятельных заданий.

6.2. Рекомендации по организации самостоятельной работы

Самостоятельная работа включает изучение литературы, поиск информации в сети Интернет, подготовку к тестам, экзамену. Необходимо разобраться в основных понятиях. Записать возникшие вопросы и найти ответы на них на занятиях, либо разобрать их с преподавателем. Подготовка к экзамену необходимо начинать заранее.

Следует проанализировать научный и методический материал учебников, учебно-методических пособий, конспекты лекций. Знать формулировки терминов и уметь их четко воспроизводить.

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
6	ПК-9	Отчет по практическим работам №№1-13
		Вопросы к зачету №№1-40
		Б

7.2. Типовые задания или иные материалы, необходимые для текущего контроля

7.2.1. Практическая работа

(наименование оценочного средства)

- Практическая работа 1 Хронологии развития социальной инженерии
- Практическая работа 2 Оценка личной уязвимости к социальной инженерии
- Практическая работа 3 Принципы влияния Р. Чалдини в социальной инженерии
- Практическая работа 5 Анализ специализированных OSINT-инструментов: классификация, функционал и сценарии применения
- Практическая работа 6 Моделирование цикла атаки Hadnagy
- Практическая работа 7 Введение в Sherlock: автоматизированный поиск аккаунтов по никнейму
- Практическая работа 8 Визуальный OSINT-анализ с Maltego Community Edition
- Практическая работа 9. Автоматизация OSINT-расследований с использованием больших языковых моделей (LLM): от промпт-инжиниринга до аналитического отчета»
- Практическая работа 10. Моделирование атаки Evil Twin WiFi и анализ безопасности беспроводных сетей
- Практическая работа 11. Разработка сценария комплексной атаки с использованием методов социальной инженерии
- Практическая работа 12 Анализ 50 постов о компании. Выявление уязвимостей
- Практическая работа 13. Оценка уровня защищенности организации от социальной инженерии

Типовой(ые) пример(ы) задания(ий)

Таблица 1.1 – Хронология развития социальной инженерии

Период	Ключевые события и тенденции	Представители / Источники

Период	Ключевые события и тенденции	Представители / Источники

Таблица 1.2 – Известные социальные инженеры и их атаки

Имя / Группа	Период активности	Описание и вклад	Известные атаки с использованием социальной инженерии

Темы письменных работ

№	Тема
1	Техники манипулирования людьми
2	Определение психотипа по постам в соцсетях
3	Определение технологических векторов цифровых атак на сотрудников
4	Организация и проведение фишинговой атаки
5	Кликджекинг. Спирфишинг

Краткое описание и регламент выполнения

1. Используя доступные источники информации (научные статьи, книги, публикации в СМИ и специализированных ресурсах по кибербезопасности), изучите историю развития социальной инженерии.
2. Заполните предложенную таблицу, отразив в ней хронологию развития социальной инженерии от истоков до наших дней.
3. В отдельной части таблицы укажите не менее 3-х наиболее известных социальных инженеров (или групп), опишите их вклад и наиболее известные атаки с использованием методов социальной инженерии.

Критерии оценки:

- оценка «зачтено» выставляется студенту, если практическое задание выполнено грамотно или имеет несущественные замечания, выполнен отчет по работе.
- оценка «не зачтено» выставляется студенту, если практическое задание не выполнено, имеет грубые ошибки, не подготовлен отчет.

7.2.4 Типовой пример тестового задания

Сущность социотипа Эмотив:

Выберите один или несколько вариантов ответа:

- 1) яркие эмоции
- 2) сопереживания
- 3) драматизация ситуации
- 4) впечатлительность
- 5) нерешительность

Критерии оценки:

Баллы начисляются автоматически пропорционально правильным ответам.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр 6

№	Вопросы к зачету
1	Дайте определение социальной инженерии (СИ) как вида психологической манипуляции. В чем заключаются ее научные основы (связь с психологией, социологией, теорией коммуникаций)?
2	Объясните, почему методы социальной инженерии работают эффективнее многих технических атак. Назовите основные точки воздействия на человека.
3	Перечислите и охарактеризуйте основные слабости человеческой психики, которые эксплуатирует социальный инженер (доверчивость, желание помочь, страх, авторитет и др.).
4	Какие психологические принципы и стереотипы мышления (эвристики) чаще всего используются при планировании атак? Приведите примеры.
5	Назовите основные мотивы и страхи жертвы, на которые давит злоумышленник. Как знание этих мотивов помогает в построении атаки?
6	Опишите базовые модели социальной инженерии (например, модель К. Хэднаги) и объясните их практическое применение.
7	Каковы основные способы защиты личности и организации от социальной инженерии на психологическом уровне?
8	Составьте краткую хронологию развития социальной инженерии как вида киберугроз (ключевые этапы, известные атаки, эволюция методов).
9	Как провести оценку собственной личной уязвимости к методам социальной инженерии? Какие факторы повышают риск стать жертвой?

№	Вопросы к зачету
10	Перечислите и раскройте 6 принципов влияния по Р. Чалдини. Для каждого приведите пример использования в социальной инженерии.
11	Что такое разведка (reconnaissance) в контексте социальной инженерии? Какие цели она преследует и на какие этапы делится?
12	Дайте определение OSINT. Как OSINT-методы используются для сбора информации о жертве перед атакой?
13	Что такое «цифровой след человека»? Из каких компонентов он состоит (соцсети, форумы, утечки данных, геолокация и т.д.)?
14	Назовите и классифицируйте основные типы OSINT-инструментов (по назначению: поиск по нику, по email, по фото, анализ связей).
15	Опишите функционал и сценарии применения таких OSINT-инструментов, как Sherlock, Maltego, theHarvester, Recon-ng.
16	Объясните, как работает инструмент Sherlock. Какую задачу он решает и в чем его ограничения?
17	Как проводится визуальный OSINT-анализ с использованием Maltego Community Edition? Что такое «трансформы» и как они работают?
18	Опишите цикл атаки по модели Хэднаги (Hadnagy). Из каких этапов он состоит и чем отличается от традиционных моделей кибератак?
19	Как большие языковые модели (LLM) могут быть использованы для автоматизации OSINT-расследований? Приведите примеры промптов.
20	Что такое промпт-инжиниринг в контексте OSINT? Как с его помощью можно повысить эффективность сбора данных?
21	Дайте определение фишинга (phishing). Каковы основные виды фишинговых атак (массовый, целевой, гарпунный, китобойный)?
22	Что такое вишинг (vishing) и смишинг (smishing)? В чем их особенности по сравнению с email-фишингом?
23	Опишите технологию атаки Evil Twin WiFi. Как злоумышленник создает поддельную точку доступа и какие цели преследует?
24	Как проводится моделирование атаки Evil Twin WiFi в лабораторной среде? Какие инструменты для этого используются?
25	Что такое «дубликат аккаунта» (клон) и «захват аккаунта» (takeover)? Какие методы социальной инженерии для этого применяются?

№	Вопросы к зачету
26	Как дипфейки (deepfakes) и ИИ-инструменты (голосовые и видео-синтезаторы) усиливают эффективность социальной инженерии?
27	Опишите методы физического проникновения (pretexting, tailgating, piggybacking, impersonation). Приведите примеры легенд.
28	Разработайте сценарий комплексной атаки с использованием методов социальной инженерии (от сбора информации до достижения цели).
29	Назовите основные способы противодействия методам социальной инженерии на организационном уровне (политики, процедуры).
30	Какие технические средства защиты помогают снизить риски социальной инженерии (фильтрация, антифишинг, MFA, DLP)?
31	Как проводится анализ постов компании в соцсетях для выявления уязвимостей? Какие данные можно извлечь и использовать в атаке?
32	Каковы юридические аспекты подготовки легитимной атаки (пентеста) методами социальной инженерии? Что такое HTA (Handling Authorization)?
33	Что такое профайлинг (profiling) в контексте социальной инженерии? Какие характеристики жертвы подлежат анализу?
34	Опишите методологию подготовки и проведения легитимной атаки социальной инженерии (этапы, роли, документирование).
35	Как проводится тестирование инструментов социальной инженерии перед реальной атакой? Какие риски нужно учитывать?
36	Какова структура отчета по итогам проведения атаки социальной инженерии? Какие разделы обязательны?
37	Как результаты тестирования на проникновение методами социальной инженерии используются для повышения осведомленности сотрудников?
38	Опишите процедуру оценки уровня защищенности организации от социальной инженерии (методика, KPI, этапы).
39	Какие программы повышения осведомленности (Security Awareness) наиболее эффективны для защиты от социальной инженерии?
40	Приведите пример реальной успешной атаки социальной инженерии (известные кейсы). Проанализируйте, какие методы были использованы и как можно было защититься.

7.3.2. Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
6	Зачет (письменно/по накопительному рейтингу)	«зачтено»	55-100 баллов
		«не зачтено»	0-54 баллов

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
6	Зачет	«зачтено»	практические работы выполнены грамотно или имеют несущественные замечания; обучающийся владеет теоретическим материалом, отвечает на дополнительные вопросы
		«не зачтено»	практические работы не выполнены или имеют существенные замечания; обучающийся не владеет теоретическим материалом, не отвечает на дополнительные вопросы или отвечает с грубыми ошибками

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Жемерикина, Ю. И.	Социальная инженерия. Практикум : учебное пособие / Ю. И. Жемерикина, Т. А. Талалуева. — Москва : РТУ МИРЭА, 2022. — 82 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/310898	учебное пособие	2022	Лань : электронно-библиотечная система
2	Хэднеги, К.	Искусство обмана: Социальная инженерия в мошеннических схемах : практическое руководство / К. Хэднеги. - Москва : Альпина Паблишер, 2026. - 432 с. - ISBN 978-5-9614-1072-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2235297	практическое руководство	2026	ЭБС «ZNANIUM»

8.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Романов, В. Г.	Социальная инженерия мошенничества : монография / В. Г. Романов, И. В. Романова. — Чита : ЗабГУ, 2021. — 240 с. — ISBN 978-5-9293-2771-1. — Текст : электронный// Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/271808	монография	2020	Лань : электронно-библиотечная система

8.3. Перечень профессиональных баз данных и информационных справочных систем

№ пп	Наименование	Ссылка
1	Springer Nature (Полнотекстовая коллекция журналов)	https://www.springernature.com/gp/products
2	Springer eBooks (Полнотекстовая коллекция электронных книг издательства Springer Nature)	https://link.springer.com/
3	«Кодекс»	https://kodeks.ru/
4	Техэксперт	https://cntd.ru/

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Windows	Windows (Договор № 690 от 19.05.2015г., срок действия - бессрочно);
2	OfficeStandart	OfficeStandart (Договор № 690 от 19.05.2015г., срок действия - бессрочно; Договор № 727 от 20.07.2016г., срок действия - бессрочно)
3.	Консультант+	Консультант+ (Договор №1522 от 25.12.2015, срок действия - бессрочно)

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Помещение для самостоятельной работы обучающихся Д -409	Стол-парты двухместные, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор, компьютерные столы, компьютеры для студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф
2	Помещение для самостоятельной работы обучающихся Г-401	Стол, стулья, компьютеры
3	Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для	Стол учебный двухместный, стулья, стол преподавательский, стул преподавательский, доска аудиторная (меловая), кафедра напольная

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
	проведения занятий, текущего контроля и промежуточной аттестации. Д-402	
4	Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий, текущего контроля и промежуточной аттестации. Д-413	Столы ученические двухместные, стулья, стол преподавательский, стул преподавательский, доска аудиторная (меловая) , кафедра напольная
5	Лаборатория кибербезопасности. Лаборатория «Автоматизированные системы в защищенном исполнении». Лаборатория «Программно-аппаратные средства защиты информации». Лаборатория «Безопасность вычислительных сетей» Лаборатория «Техническая защита информации». Лаборатория «Сети и системы передачи информации». Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для научно-исследовательской работы обучающихся, курсового и дипломного проектирования. Аудитория для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну Э-101в	Столы компьютерные, стол преподавательский, стулья, шкаф металлический, телевизор на передвижной тумбе, стойка телекоммуникационная, коммутатор оптический Qtech QSW-6910-26F, коммутатор Qtech QSW-4610-28T-AC, система хранения данных Русский щит Alpha DF5045, сервер Русский щит Gamma SX6302, ноутбук Digma Pro Sprint M DN15P3-8CXW02, осциллограф АКИП-4115/1А, анализатор низкочастотных сигналов СКМ-21, генератор сигналов АКИП-3407/1А, антенна дипольная активная Е-3000А1, антенна рамочная Н-30А1, акустический излучатель АС-1 Лайт Арт.001, рефлектометр ТОПАЗ-7317-ARX, измерительный пробник напряжения ШИП, анализатор спектра АКИП-4211/1, межсетевой экран ССПТ-2